1. Program studiów

Nazwa studiów podyplomowych	**Audytor Tożsamości Cyfrowej**
Poziom Polskiej Ramy Kwalifikacji	**7**
Liczba semestrów	**2**
Liczba godzin zajęć	**174**
Liczba punktów ECTS konieczna dla ukończenia studiów podyplomowych	**30**
Forma zakończenia studiów podyplomowych	praca końcowa
Cel studiów. Opis uprawnień absolwenta związanych z posiadaną kwalifikacją	Celem studiów podyplomowych na kierunku Audytor Tożsamości Cyfrowej jest przygotowanie absolwentów do pełnienia roli eksperta w zakresie prowadzenia zaawansowanych analiz z jawnych źródeł (OSINT) oraz realizacji audytów tożsamości cyfrowej osób, organizacji i innych podmiotów. Program kształcenia ukierunkowany jest na rozwój kompetencji w zakresie pozyskiwania, integrowania i analizy danych z otwartych źródeł, identyfikacji i weryfikacji tożsamości cyfrowej, oceny wiarygodności podmiotów oraz rozpoznawania i analizy ryzyk związanych z nadużyciami tożsamości. Uczestnikami studiów mogą być osoby, które: – są zatrudnione lub planują podjąć pracę w instytucjach obowiązanych (np. banki, instytucje finansowe, fintech, ubezpieczenia, biura rachunkowe) lub – pracują w obszarach compliance, AML, audytu, kontroli lub zarządzania ryzykiem lub – wykonują zawody prawnicze lub finansowe (np. adwokaci, radcowie prawni, doradcy podatkowi, biegli rewidenci) lub – są pracownikami administracji publicznej lub instytucji nadzorczych oraz pracownicy sektora prywatnego. Absolwent studiów jest specjalistą w zakresie prowadzenia analiz OSINT oraz weryfikacji tożsamości cyfrowej. Potrafi pozyskiwać, integrować i analizować dane z różnych źródeł w celu oceny wiarygodności oraz identyfikacji zagrożeń, w tym związanych z cyberprzestępczością, dezinformacją i wyciekami danych. Projektuje i realizuje procesy analityczne i operacyjne, dobiera metody i narzędzia pracy oraz formułuje

	wnioski i rekomendacje na podstawie przeprowadzonych analiz. Przygotowuje raporty analityczne i prezentuje wyniki w sposób wspierający podejmowanie decyzji, działając zgodnie z zasadami etyki oraz podejściem opartym na analizie ryzyka. Studia przygotowują do stosowania podejścia opartego na analizie ryzyka zgodnie z normą ISO 42001 oraz do przystąpienia do egzaminu certyfikacyjnego w zakresie zarządzania ryzykiem.
Zasady rekrutacji	Na studia mogą zostać zakwalifikowani kandydaci, którzy: 1) w terminie naboru zapiszą się na studia podyplomowe poprzez system Internetowej Rejestracji Kandydatów (IRK), wypełnią formularz zgłoszeniowy i wgrają wymagane dokumenty: a. skan dyplomu ukończenia studiów wyższych; b. CV w języku polskim (uwzględniające przebieg zatrudnienia, wraz ze wskazaniem miejsca i czasu zatrudnienia oraz zajmowane stanowiska); c. list motywacyjny; d. klauzula RODO. O przyjęciu na studia podyplomowe decyduje kolejność zgłoszeń (dzień i godzina zgłoszenia).
Wymiar, zasady i forma odbywania praktyk	Nie dotyczy

2. Opis efektów uczenia się

Efekty uczenia się w zestawach				
Symbol efektu uczenia się	**Efekt uczenia się**	**Symbol kryterium weryfikacji**	**Kryterium weryfikacji**	**Odniesienie do efektów uczenia się na poziomie 7 PRK**
Projektowanie systemu OSINT (Open Source Intelligence)				
ATC_W1	Opisuje architekturę systemu OSINT wraz z jego kluczowymi elementami	W1_1	definiuje cel działania systemu OSINT oraz charakteryzuje jego elementy składowe	P6S_WG
		W1_2	opisuje logiczną architekturę systemu OSINT	
		W1_3	identyfikuje źródła danych OSINT	
		W1_4	przedstawia przepływ danych pomiędzy elementami systemu	
ATC_W2	Opisuje regulacje prawne i kwestie etyczne audytu cyfrowego	W2_1	opisuje kontekst prawny, organizacyjny i etyczny powiązany z OSINT	P6S_WK
		W2_2	opisuje procedurę przeprowadzania audytu i postępowań audytowych	
ATC_U1	Ocenia legalność pozyskiwania i przetwarzania danych w audycie oraz postępowaniach, a także projektuje, standaryzuje i wdraża proces audytu OSINT zgodnie z obowiązującymi normami, procedurami i wymaganiami prawnymi	U1_1	analizuje zgodność procesu pozyskiwania i przetwarzania danych z obowiązującymi przepisami prawa oraz zasadami etyki audytu	P7S_UW
		U1_2	projektuje procedury audytu OSINT zgodnie z obowiązującymi normami i standardami organizacyjnymi	
		U1_3	standaryzuje przebieg procesu audytu OSINT z wykorzystaniem określonych procedur i dokumentacji	
		U1_4	wdraża proces audytu OSINT zgodnie z wymaganiami prawnymi, organizacyjnymi i bezpieczeństwa informacji	
ATC_U2	Prowadzi działalność operacyjną w sposób twórczy,	U2_1	dobiera innowacyjne rozwiązania OSINT adekwatne do celu i charakteru działań operacyjnych	P7Z_UN

	poszukuje alternatywnych rozwiązań i zarządza tożsamością przybraną	U2_2	dobiera działania minimalizujące zagrożenia w działalności operacyjnej adekwatnie do charakteru sytuacji operacyjnej	
		U2_3	stosuje zasady zarządzania tożsamością przybraną w celu zapewnienia bezpieczeństwa działań operacyjnych	
		U2_4	dostosowuje metody działania do zmieniających się warunków operacyjnych w celu osiągnięcia założonych celów	
		U2_5	rozwija techniki i systemy separacji środowisk	
Projektowanie i modyfikowanie procesów operacyjnych i analiza				
ATC_U3	Dobiera techniki zbierania informacji w celu identyfikacji procesów wywiadowczych	U3_1	identyfikuje cel zbierania informacji oraz kontekst procesu wywiadowczego	P7S_UW
		U3_2	uzasadnia wybór technik, odwołując się do ich skuteczności, zakresu pozyskiwanych danych i dostępności źródeł	
		U3_3	opracowuje schemat interwencji, w tym definiuje ślad cyfrowy	
		U3_4	rozwija elementy analizy behawioralnej użytkowników	
ATC_U4	Analizuje ogólnodostępne rejestry w celu identyfikacji przebiegu procesów organizacyjnych / biznesowych	U4_1	identyfikuje ogólnodostępne rejestry i źródła danych	P7Z_UI
		U4_2	pozyskuje dane z ogólnodostępnych rejestrów w sposób zgodny z ich strukturą i zasadami dostępu	
		U4_3	tworzy mapy struktur powiazań gospodarczych	
		U4_4	wykrywa niespójności, luki informacyjne lub nietypowe zmiany w przebiegu procesu na podstawie danych rejestrowych	
ATC_U5	Wizualizuje wyniki analizy danych	U5_1	dokonuje weryfikacji zdjęć, audio i wideo	P7S_UK
		U5_2	dobiera typ wizualizacji do rodzaju i struktury danych oraz celu analizy	
		U5_3	prezentuje wyniki analizy w formie graficznej umożliwiającej interpretację zależności, trendów lub anomalii	
		U5_4	interpretuje przedstawione wizualnie wyniki, formułując wnioski analityczne	

ATC _W3	Charakteryzuje ekosystem finansowy, jego elementy, funkcje oraz zależności pomiędzy uczestnikami rynku w kontekście analizy OSINT	W3_1	definiuje ekosystem finansowy wraz z jego elementami i funkcjami	P6Z_WZ
		W3_2	charakteryzuje rolę instytucji, podmiotów i narzędzi występujących w ekosystemie finansowym	
ATC _U6	Tworzy modele ekosystemu finansowego w analizie OSINT	U6_1	rozpoznaje źródła danych finansowych oraz instytucje je tworzące	P7S_UW
		U6_2	tworzy zasady bezpieczeństwa systemu dla organizacji	
Analiza danych oraz działalność operacyjna				
ATC _U7	Ocenia działalność finansową w oparciu o pogłębioną analizę danych	U7_1	pozyskuje i przetwarza informacje finansowe o podmiotach gospodarczych i osobach fizycznych	P7Z_UI
		U7_2	interpretuje możliwości finansowe podmiotów gospodarczych	
		U7_3	interpretuje wyniki analizy danych finansowych i niefinansowych	
ATC _U8	Analizuje infrastrukturę internetową	U8_1	wyszukuje źródła danych technicznego wywiadu	P6Z_UW
		U8_2	identyfikuje zagrożenia związane z infrastrukturą internetową	
		U8_3	pozyskuje informacje o infrastrukturze internetowej z wykorzystaniem ogólnodostępnych źródeł i narzędzi analitycznych	
ATC _U9	Dobiera metody i narzędzia w celu identyfikacji cyberprzestępczości finansowej	U9_1	identyfikuje podstawowe formy cyberprzestępczości finansowej	P6S_UW
		U9_2	stosuje dobrane metody i narzędzia w analizie przypadku lub scenariuszu symulowanym	
		U9_3	rozpoznaje procesy polegające na praniu pieniędzy	
ATC _U10	Operacjonalizuje działania i analizuje wyciek danych	U10_1	określa cel analizy wycieku danych oraz zakres operacjonalizacji działań	P7Z_UO
		U10_2	identyfikuje skalę, zakres i potencjalne konsekwencje wycieku danych dla organizacji lub interesariuszy	
		U10_3	ocenia skuteczność działań oraz zgodność z przyjętymi założeniami i standardami audytu	

Wnioskowanie oraz prezentacja uzyskanych danych				
ATC _U11	Tworzy modele przeciwdziałania dezinformacji	U11_1	identyfikuje interesariuszy oraz aktorów uczestniczących w procesach dezinformacyjnych	P7S_UW
		U11_2	wykrywa treści manipulacyjne	
		U11_3	dobiera metody i techniki przeciwdziałania dezinformacji adekwatne do zidentyfikowanych mechanizmów	
ATC _U12	Dokonuje automatyzacji procesów OSINT	U12_1	kreuje i nadzoruje automatyzację pracy poprzez zbieranie, filtrowanie i wstępną analizę danych	P7Z_UN
		U12_2	identyfikuje ryzyka i ograniczenia automatyzacji procesów OSINT	
		U12_3	ocenia efektywność automatyzacji w odniesieniu do czasu, jakości danych i powtarzalności procesu	
ATC _U13	Raportuje i tworzy wizualizacje powiązań	U13_1	identyfikuje dane i relacje wymagające zaprezentowania w formie raportu i wizualizacji powiązań	P7S_UK
		U13_2	strukturyzuje dane w sposób umożliwiający analizę relacji i zależności	
		U13_3	opracowuje raport z audytu zawierający wyniki analizy, ocenę oraz rekomendacje	
ATC _U14	Projektuje podejście badawcze i analityczne w OSINT	U14_1	charakteryzuje metody prowadzenia analiz i opracowań eksperckich w obszarze OSINT	P7S_UW
		U14_2	formułuje problem analityczny, cele analizy oraz pytania badawcze	
		U14_3	dobiera metody i narzędzia analityczne adekwatne do problemu i dostępnych danych	
ATC _U15	Opracowuje raport analityczny/opracowanie eksperckie	U15_1	interpretuje i porządkuje wiedzę teoretyczną i praktyczną właściwą dla analizowanego problemu	P7S_UW
		U15_2	pozyskuje, ocenia i wykorzystuje źródła informacji w analizie problemu	
		U15_3	formułuje wnioski i rekomendacje na podstawie przeprowadzonej analizy	

2.1 Opis planów studiów podyplomowych

lp	semestr	Nazwa przedmiotu/modułu zajęć	Liczba godzin	Forma zajęć	Liczba ECTS	Odniesienie do efektów uczenia się na studiach podyplomowych (należy podać symbole efektów uczenia się wg kryteriów z tabeli 2.2)	Sposób weryfikacji efektów uczenia się	Nadkład pracy studenta
MODUŁ TEMATYCZNY I. Znajomość funkcjonowania systemu i polityki w zakresie bezpieczeństwa oraz odporności infrastruktury krytycznej w ramach współczesnego środowiska bezpieczeństwa								
1	1	Architektura procesu OSINT i cykl wywiadowczy	5	wykład (zajęcia online)	1	W1_1, W1_2, W1_3, W1_4	test wiedzy online, analiza przypadku, aktywność podczas zajęć	Zajęcia z wykładowcą – 5h Przygotowanie do zajęć – 6h Analiza literatury przedmiotu – 8h Konsultacje – 1h Przygotowanie do zaliczenia – 5h
2	1	Prawne i etyczne aspekty audytu tożsamości cyfrowej	5	wykład (zajęcia online)	1	W2_1, W2_2, U1_1, U1_2, U1_3, U1_4	test wiedzy online, analiza przypadku (legalność działań); udział w dyskusji	Zajęcia z wykładowcą – 5h Analiza aktów prawnych i literatury – 8h Przygotowanie do zajęć – 6h Konsultacje – 1h Przygotowanie do zaliczenia – 5h
3	1	OPSEC (Operation Security) i zarządzanie tożsamością przybraną	10	warsztat	2	U2_1, U2_2, U2_3, U2_4, U2_5	zadanie praktyczne (strategia opsec); symulacja operacyjna; projekt indywidualny	Zajęcia z wykładowcą – 10h Przygotowanie do zajęć praktycznych – 10h Czytanie literatury specjalistycznej – 10h Przygotowanie prac cząstkowych – 12h Konsultacje – 2h Przygotowanie do zaliczenia – 6h
4	1	Zaawansowane techniki wyszukiwania i SOCMINT	10	warsztat	2	U3_1, U3_2, U3_3, U3_4	zadania praktyczne (wyszukiwanie i analiza danych); test umiejętności	Zajęcia z wykładowcą – 10h Ćwiczenia praktyczne – 15h Analiza literatury przedmiotu – 5h Przygotowanie analiz cząstkowych – 8h Konsultacje – 2h Przygotowanie do zaliczeni – 10h

5	1	Analiza rejestrów publicznych, korporacyjnych i UBO	10	konwersatorium	1	U4_1, U4_2, U4_3,U4_4	case study; stworzenie raportu analitycznego	Zajęcia z wykładowcą – 10h Przygotowanie do zajęć – 8h Konsultacje – 1h Przygotowanie do zaliczenia – 6h
6	1	Wizualna analiza danych, GEOINT i metadane	10	warsztat	2	U5_1, U5_2, U5_3, U5_4	projekt (wizualizacja danych), prezentacja	Zajęcia z wykładowcą – 10h Ćwiczenia praktyczne – 15h Analiza literatury przedmiotu – 5h Przygotowanie analiz cząstkowych – 8h Konsultacje – 2h Przygotowanie do zaliczeni – 10h
7	1	Ekosystem finansowy w analizie OSINT	10	konwersatorium	1	U6_1, U6_2	test wiedzy; analiza przypadku	Zajęcia z wykładowcą – 10h Analiza literatury przedmiotu – 5h Przygotowanie do zajęć – 3h Przygotowanie do zaliczenia – 5h
8	1	Analiza danych finansowych (FININT)	10	konwersatorium (zajęcia online)	1	U7_1, U7_2, U7_3	test wiedzy online; zadania analityczne; raport finansowy	Zajęcia z wykładowcą – 10h Analiza literatury przedmiotu – 5h Przygotowanie do zajęć – 3h Przygotowanie do zaliczenia – 5h
9	1	Biały wywiad techniczny i analiza infrastruktury internetowej	10	warsztat	2	U8_1, U8_2, U8_3	zadanie praktyczne; test wiedzy	Zajęcia z wykładowcą – 10h Ćwiczenia praktyczne – 15h Analiza literatury przedmiotu – 5h Przygotowanie analiz cząstkowych – 8h Konsultacje – 2h Przygotowanie do zaliczeni – 10h
10	1	Kryptowaluty i cyberprzestępczość finansowa	10	konwersatorium (zajęcia online)	2	U9_1, U9_2, U9_3	test wiedzy, case study	Zajęcia z wykładowcą – 10h Ćwiczenia praktyczne – 15h Analiza literatury przedmiotu – 5h Przygotowanie analiz cząstkowych – 8h Konsultacje – 2h Przygotowanie do zaliczeni – 10h
11	2	Śledztwa w Dark Webie i analiza wycieków danych	10	konwersatorium	1	U10_1, U10_2, U10_3	śledztwa w dark webie i analiza wycieków danych	Zajęcia z wykładowcą – 10 h Analiza literatury przedmiotu – 5h Przygotowanie do zajęć – 3h Przygotowanie do zaliczenia – 5h
12	2	Przeciwdziałanie dezinformacji i weryfikacja autentyczności profili	10	wykład (zajęcia online)	2	U11_1, U11_2, U11_3	test, analiza problemowa, prezentacja krótkiej analizy	Zajęcia z wykładowcą – 10h Analiza literatury przedmiotu – 5h Przygotowanie do zajęć – 3h Przygotowanie do zaliczenia – 5h

13	2	Automatyzacja procesów OSINT i zastosowanie AI	10	konwersatorium (zajęcia online)	2	U12_1, U12_2, U12_3	test wiedzy online; projekt techniczny	Zajęcia z wykładowcą – 10h Ćwiczenia praktyczne – 15h Analiza literatury przedmiotu – 5h Przygotowanie analiz cząstkowych – 8h Konsultacje – 2h Przygotowanie do zaliczeni – 10h
14	2	Raportowanie wywiadowcze i wizualizacja powiązań	10	warsztat	2	U13_1, U13_2, U13_3;	raport końcowy prezentacja	Zajęcia z wykładowcą – 10h Ćwiczenia praktyczne – 15h Analiza literatury przedmiotu – 5h Przygotowanie analiz cząstkowych – 8h Konsultacje – 2h Przygotowanie do zaliczeni – 10h
15	2	Metodyka pisania pracy końcowej	10	seminarium	2	U14_1, U14_2, U14_3	przygotowanie koncepcji pracy końcowej, prezentacja założeń pracy, ocena projektu metodologicznego	Zajęcia z wykładowcą – 10h Ćwiczenia praktyczne – 15h Analiza literatury przedmiotu – 5h Przygotowanie analiz cząstkowych – 8h Konsultacje – 2h Przygotowanie do zaliczeni – 10h
16	2	Seminarium	10	seminarium	3	U15_1, U15_2, U15_3	przygotowanie pracy końcowej, prezentacja pracy końcowej, obrona pracy końcowej	Zajęcia z wykładowcą – 10h Przygotowanie projektu – 30h Analiza źródeł – 8h Konsultacje i przygotowanie prezentacji – 6h
17	2	Zarządzanie ryzykiem wg normy ISO 42001, egzamin Menadżer ds. zarządzania sztuczna inteligencją (AIMS)	10	wykład	1	U2_1, U2_2, U2_3, U8_2, U8_3	test wiedzy, analiza przypadku zarządzania ryzykiem	Zajęcia z wykładowcą – 10h Analiza norm i materiałów – 6h Przygotowanie zadania – 5h Przygotowanie do zaliczenia – 4h
18	2	Zarządzanie ryzykiem wg normy ISO 42001, egzamin Menadżer ds. zarządzania sztuczna inteligencją (AIMS)	14	konwersatorium	2	U2_1, U2_2, U2_3, U8_2, U8_3	projekt systemu zarządzania ryzykiem, analiza skuteczności działań	Zajęcia z wykładowcą – 14h Ćwiczenia praktyczne – 12h Przygotowanie projektu – 16h Analiza materiałów – 6h Przygotowanie do zaliczenia – 2h

zajęcia teoretyczne: wykłady
zajęcia praktyczne: konwersatoria, warsztaty, seminaria

Warunkiem otrzymanie świadectwa ukończenia studiów podyplomowych jest osiągnięcie pozytywnych wyników z wszystkich wymaganych programem przedmiotów oraz napisanie pracy końcowej.